MODELING POWER NON-RECOVERY USING THE SAPHIRE RISK ASSESSMENT SOFTWARE

Curtis L. Smith[1], John A. Schroeder[1], Scott T. Beck[1], and James K. Knudsen[2]

[1] Bechtel BWXT Idaho, LLC.
Idaho Falls, Idaho 83415
[2] Bechtel SAIC, LLC.
Las Vegas, Nevada 89144

ABSTRACT

SAPHIRE (Systems Analysis Program for Hands-on Integrated Reliability Evaluation) is a software tool for performing probabilistic risk assessments. Within this tool, there exists the capability to create and quantify logic models depicting a nuclear power plant's response to an accident, including the potential for recovery of failed components. Specifically we discuss two methods of incorporating these "nonrecovery" basic events into the risk model via (1) the direct manipulation of the logic structure or (2) the application of "recovery" rules. Also presented are three methods of quantifying the nonrecovery probabilities, including general human reliability analysis, integration of the recovery times, and a "time series" Monte Carlo simulation approach. The results of our analysis show that introducing offsite power recovery events into the model is relatively simple. But, determining the appropriate probabilities (conditional upon specific accident sequences) is generally a non-trivial process. With the aid of time-based recovery modules in SAPHIRE, the determination of applicable nonrecovery probabilities becomes a manageable process.

KEYWORDS

Recovery, accident, human, SAPHIRE, PRA, risk, reliability

INTRODUCTION

In a probabilistic risk assessment (PRA), cut sets for accident sequences are generated using the fault tree and event tree logic. Since most PRAs are analyzed in failure space, a cut set represents the minimal set of components or systems that have to fail (given a particular initiating event) in order to result in an undesired condition (e.g., core damage). As part of an accident sequence, operator actions that could prevent the accident sequence from progressing to the point of an accident should be factored into the results. In general, there are two methods of including the operator nonrecovery (i.e., the probability that the operator does not restore the system or component). First, one may include the nonrecovery as part of the logic models (fault or event trees). Second, one may want to append recovery events to the accident

cut sets, where recovery rules modify the cut sets after they have been generated from the logic models.

A recovery event represent the probability that the operator or operators fail to successfully prevent the accident by restoring one or more of failed components in the sequence cut sets. Consequently, the recovery events are frequently called the nonrecovery probability events. Human reliability analysis is generally needed to quantify these nonrecovery probabilities for a particular accident sequence. Several texts discuss the analysis technique of human reliability and recovery modelling and are useful when quantifying these nonrecovery probabilities. (Swain and Guttman, 1983; Gertman and Blackman, 1994)

In a PRA, the nonrecovery events are intended to cover the general case of a component failing at any time during the mission time defined for the analysis. Consequently, the nonrecovery probability is an "average" type of value (with associated variability as defined by the uncertainty distribution) and may not be specific to a particular failure. If an analyst then wants to use the PRA to perform a calculation (for example, to obtain a conditional core damage probability), the analyst may focus on a particular configuration which may invalidate the predefined nonrecovery probability. Thus, there is the need to be able to not only calculate general nonrecovery values, but also context-specific ones. In this paper, we present three methods of calculating the nonrecovery probabilities as an aid to the reader for their own analyses, but other methods are available. (Gertman and Blackman, 1994; Fujita, 1992)

INCORPORATING NONRECOVERY EVENTS INTO THE PRA

Recovery actions in the form of operator actions can be added into SAPHIRE by directly adding them into the event tree structure as "system top events". These recovery top events account for the ability to recover the various system or systems that are effected by the initiating event or have failed to function during the event scenario. For example, loss of offsite power (LOOP) non-recovery methods for different type losses can be entered in the event tree as system top events before other specific plant responses (such as secondary side cooling) that are dependent on offsite ac power.

Recovery actions can also be added directly into the PRA fault trees. For example, during a station blackout scenario, a recovery action for an operator to recover a diesel generator that has failed to start could be added to a fault tree under an AND gate along with the "diesel generator fails to start" basic event. Human reliability worksheets (described later) could be used to obtain the operator non-recovery probability for a "operator fails to recover diesel generator" basic event.

A second method to introduce recovery actions into SAPHIRE is with the use of recovery rules. Recovery rules are "rule-based" programmatic heuristics that allow for the alteration or deletion of fault tree or sequence cut sets. Recovery actions represented as simple basic events are added onto a cut set if a user-specified search criterion is met. If a specified basic event(s) is found within a cut set, the rule will then manipulate that cut set. One such cut set manipulation that could be performed would be to append a recovery event onto the cut set. For example, if a diesel generator fails to start (EPS-DGN-FS-1A) and diesel generator 1B fails to start (EPS-DGN-FS-1B), then there is a recovery action to start a diesel generator (EPS-DGN-REC). For this type of recovery, the following recovery rule can used:

```
if EPS-DGN-FS-1A * EPS-DGB-FS-1B then
  recovery = EPS-DGN-REC;
endif
```

This recovery rule would search the cut sets within SAPHIRE and look for any cut sets meeting the search criterion of failure of both diesel generators. If the search criterion were met, the rule would append the recovery event EPS-DGN-REC to the cut set. (Russell et al., 1999) Now, one must determine the nonrecovery probability, which is generally a nontrivial activity.

DETERMINING NONRECOVERY PROBABILITIES

In this section, we will present several potential methods for determining nonrecovery probabilities. The methods range from the simple (expert judgment) to the complicated (convolution integrals). Final use of a probability determination method is, of course, left to the judgment of the reader. In general though, we will presented three methods to quantify the nonrecovery probabilities, including:

1. General human reliability analysis
2. Convolution integration of the recovery times
3. "Time series" Monte Carlo simulation

General Human Reliability Analysis

General nonrecovery probabilities can be calculated in a variety of ways. One method is the time reliability correlation (TRC) while a second method uses task- and performance factor-oriented worksheets.

First, the TRC allows for nonrecovery to be quantified based on the accident sequence timing (in response to an event) and the type of action being evaluated. (Dougherty and Fragola, 1988) For this method, a curve is used based on a set of parameters that deal with response time and performance shaping factors. The operator actions consider whether the event is covered by procedures or training. Also, one accounts for hesitancy due to conflict, burden, or uncertainty. The equation used for the TRC in order to calculate the probability of an operator failing to recover from an event for which the time available is t_a minutes is

$$P(nonrecovery) = 1 - \Phi\left(\frac{\ln(t_a) - m}{\sigma}\right) \qquad (1)$$

where Φ is the area under the normal distribution curve, m = ln(median recovery time), and σ = ln(recovery time lognormal error factor)/1.645. (Swain and Guttman, 1983)

One advantage of using the TRC method is the ability to use time in the non-recovery probability calculation. The method allows for timing issues to drive the probability of non-recovery.

The second general method for nonrecovery analysis is the human reliability worksheets utilized in the U.S. Nuclear Regulatory (NRC) SPAR models. These worksheet starts with the question “is the operator action a diagnosis or an action?” The diagnosis worksheet then begins with a probability of 1.0E-2 while the action worksheet uses a probability of 1.0E-3. The analyst must then determine of the operator has to stop at diagnoses or stop at performing the recovery action.

If the nonrecovery requires diagnosis, there is a list of task-related questions, the answer to each then affects task-specific weight factors. The diagnosis event then can range in probability from 1.0 to 1.0E-5, where the only way the low probability is realized is when ample time is available AND the operators are well trained, with excellent procedures, are fit for duty, and the plant has excellent ergonomics. If the operator nonrecovery is an action type, then the analyst must answer similar questions as those for the diagnosis analysis.

The advantages of the SPRA worksheet approach are the ability to take into consideration timing issues

along with the processes required for the specific operation based on the sequence of events. The worksheet allows for flexibility on determining the final human error probability based on the type of operator action, plant procedures for the event in question, and training.

Convolution Integration of Recovery Times

Loss of ac power is modeled in PRA event trees such as LOOP and station blackout. For example, in the case of a potential station blackout, the start of the scenario is a LOOP followed by a loss of emergency power. So, at time t=0, we consider offsite power to be unavailable. It is the responsibility of the operators to recover either offsite power (if possible) or onsite emergency power (if lost). Thus, one way to have core damage from the station blackout scenario is from (1) seeing a LOOP, (2) losing emergency power, (3) not recovering ac power (short term), (4) relief valves fail, and (5) not recovering ac power (long term). The reason we need to consider ac power recovery in two time periods, short term and long term, is that nuclear power plants are designed to handle a brief period of time without any ac power. Consequently, actions in this first time period may be very different from those considered in the second period. This breakdown of the scenario into periods is a technique known as phased mission analysis.

Our task is then to quantify failure to recover ac power in the short term and in the long term. Note that the interpretation short term and long term are plant and sequence specific. But, in general, "short term" corresponds to an interval based on the time to uncover the reactor core if no safety systems function while "long term" corresponds to the station battery depletion time. In this paper, we assume that short term represent 30 minutes and long term represents 60 minutes.

The general expression for calculating an ac power nonrecovery probability is

$$P_{NRAC}(t_{long} \mid t_{short}) = P(L > t_{long} \mid L > t_{short} \ AND \ G > t_{long} \mid G > t_{short}) \quad (2)$$

where L is the duration of LOOP, G is the duration of the diesel generator unavailability, and t_{long} is a sequence dependent duration that is greater than t_{short}. This formulation implies that if LOOP and the loss of the diesel generator are longer than the maximum time (t_{long}), then we did not recover ac power.

The NRC has collected information on restoration of diesel generators. (US NRC, 1988) From this work, it was found that the median time for restoration of one diesel generator when more than one are unavailable due to independent faults is approximately four hours. When common cause failures were involved, the median repair time was shown to be between two and eight hours. We can use the recovery time to determine a diesel recovery distribution probability density function, or $f(t) = \lambda \exp(-\lambda t)$, where t is the repair time. Thus, the cumulative diesel generator recovery distribution is $F(t) = 1 - \exp(-\lambda t)$, where we assume that the repair rate is constant and repair follows a Poisson process. From the cumulative distribution, one can determine the repair rate λ since we know the median time (e.g., four hours) and, at the median time, $F(t) = 0.5$.

We now need to return to Equation 2. To determine the nonrecovery probability, one must integrate over the diesel generator recovery distribution and the offsite power recovery distribution to find the probability that time t is longer than the realized recovery time. Thus, the probability that at least one diesel generator is not recovered for some duration G is

$$P(G > t) = \int_t^{\infty} f_D(g)dg = 1 - F_D(t) = e^{-\lambda_D t} = e^{-0.693\, t/t_{DGR\text{-}50}} \quad (3)$$

The probability that offsite power will not be recovered for duration L is

$$P(L > t) = \int_t^{\infty} f_L(l)dl = 1 - F_L(t) = e^{-\alpha t^{\beta}} \quad (4)$$

where $F_L(t)$ is the density function specific to offsite power recovery. (US NRC, 1988) We can then find the general form of the ac power nonrecovery probability as

$$P_{NRAC}(t_{long} \mid t_{short}) = \frac{e^{-\alpha t_{long}^{\beta}}}{e^{-\alpha t_{short}^{\beta}}} \cdot \frac{e^{-0.693\, t_{long}/t_{DGR_{50}}}}{e^{-0.693\, t_{short}/t_{DGR_{50}}}} \quad (5)$$

where t_{DGR50} is the median diesel generator repair time. The α and β values may be found from a variety of sources. (US NRC, 1988; Minarick, 1989; Atwood et al., 1998) Note that while Equation 5 is not built into SAPHIRE itself, another code (GEM) that accompanies it does have the nonrecovery calculation as an integrated part of the model. (Russell et al., 1995)

"Time Series" Monte Carlo Simulation

The third potential method of determining the nonrecovery probability centers on Monte Carlo simulation. When one looks at recovery of ac power, we have, primarily, two competing factors. First, we have the time that it takes until undesirable outcomes occur while we are waiting for recovery of ac power. Second, we have recovery of the ac power itself. Like the previous section, if the restoration time is longer than the "maximum" time, then we do not have recovery. Consequently, we can simulate these two processes since we have a probability density function for recovery times (for example, see Equations 3 and 4) and we know, from the thermal-hydraulic features of the plant, the recovery duration of interest.

SAPHIRE has been designed to allow user-defined probability calculation modules to be used at "run time" rather than having to be compiled directly into the code base itself. These modules are assigned to basic events, called "compound events," which can then be included directly in the fault tree and event tree logic models. For one of these compound event modules, SAPHIRE has the ability to perform Monte Carlo calculations within the time domain, which fits well with our recovery scenario. We call this probability module "time series" since it simulates a series of time-based events.

Within the time series module, the user must define two items. First, SAPHIRE requests the mission time, where the mission time here would be akin to t_{long}. Second, we need the time-based event(s), where, for example, we might be interested in the diesel generator time to recover. Note that the time-based events represent times to recover (not probabilities) and, therefore, may be represented by an exponential, Weibull, or other distribution. Fortunately, SAPHIRE has a variety of distributions from which to choose.

The output for compound events using the time series simulation will be a probability representing the fraction of time recovery is greater than the mission time. For example, if we denote that the diesel generator repair rate λ is distributed exponentially, we can determine the mean time to repair since $T_{mean} = 1/\lambda$. From the earlier discussion, it was noted that the median repair time was about 4 hours, which implies that the mean repair time is 5.8 hours. Now, if our mission time is 4 hours and the time-based event is exponential with mean of 5.8 hours, we can construct our compound event.

Figure 1 shows a portion of the data entry screen and the probability that SAPHIRE determines for the nonrecovery event. In this case, when the

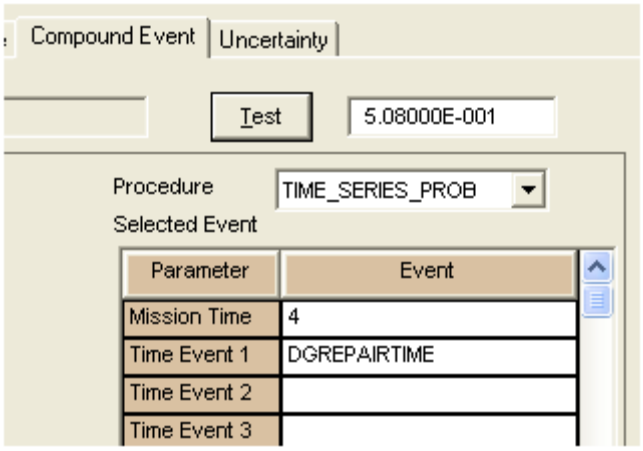

Figure 1. Portion of SAPHIRE basic event screen for the compound event development.

mean time to repair is 5.8 hours and the mission time is 4 hours, SAPHIRE estimates a nonrecovery probability of 0.508, while the exact answer is 0.500. More complicated nonrecovery events can be analyzed by introducing additional time-based parameters into the compound event structure.

RESULTS

We have discussed two methods of introducing nonrecovery events into a PRA via the logic models themselves and through the use of recovery rules. When one desires to have “cut set level” recovery modeling, the use of recovery rules becomes invaluable.

We also demonstrated three methods of quantifying the nonrecovery probabilities, including (1) general human reliability analysis, (2) integration of the recovery times, and (3) a "time series" Monte Carlo simulation. Other quantification methods are available, but the three presented provide a variety of application techniques and sophistication levels, and should be suitable for many applications.

REFERENCES

Atwood, C. L. et al, 1998. *Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980 – 1996*, NUREG/CR-5496, Idaho National Engineering and Environmental Laboratory.

Dougherty, Jr., E. M. and J. R. Fragola, 1988. *Human Reliability Analysis, A Systems Engineering Approach With Nuclear Power Plant Applications*. John Wiley & Sons, pg. 124.

Fujita, Y., 1992. *Reliability Engineering and System Safety*, “Human Reliability Analysis: A Human Point of View,” Vol 38, No. 1-2: 71-79.

Gertman, D. I. and H. S. Blackman, 1994. *Human Reliability & Safety Analysis Data Handbook*. 1st Ed. John Wiley & Sons, Inc.

Minarick, J. W., 1989. *Revised LOOP Recovery and PWR Seal LOCA Models*, ORNL/NRC/LTR-89/11.

Russell, K. D., et al., 1999. *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 6.0 System Overview Manual*, NUREG/CR-6532.

Russell, K. D. et al., 1995. *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0, Volume 6 - Graphical Evaluation Module (GEM)*, NUREG/CR-6116.

Swain, A. D., and H. E. Guttman, 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, Sandia National Laboratories.

U.S. Nuclear Regulatory Commission, 1988. *Evaluation Of Station Blackout Accidents At Nuclear Power Plants,* NUREG-1032. Washington, D.C.